

AUSA McCulley

**UNITED STATES DISTRICT COURT FOR THE
DISTRICT OF MARYLAND**

**IN THE MATTER OF THE APPLICATION OF
THE UNITED STATES OF AMERICA FOR A
WARRANT AUTHORIZING THE SEARCH OF
CERTAIN ELECTRONIC DEVICES**

Case No. 1:21-mj-2320 TMD

Filed Under Seal

**IN THE MATTER OF THE APPLICATION OF
THE UNITED STATES OF AMERICA FOR A
WARRANT AUTHORIZING THE SEARCH OF
A GOLD 2000 CHRYSLER TOWN AND
COUNTRY VAN, BEARING SOUTH
CAROLINA REGISTRATION SFR-178, VIN
1C4GP54L9YB593093**

Case No. 1:21-mj-2321 TMD

☒ FILED ☐ ENTERED
☐ LOGGED ☐ RECEIVED

Filed Under Seal

8:25 am, Sep 09 2021
AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY _____ Deputy

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Joshua Futter, a Special Agent (“SA”) with the Bureau of Alcohol, Tobacco, Firearms,
and Explosives (“ATF”), being duly sworn, depose and state as follows:

INTRODUCTION

1. This affidavit is made in support of a search warrants for:
 - a. A black iPhone contained in a clear phone case with stickers on it, belonging to Mizell TAYLOR (**SUBJECT ELECTRONIC DEVICE 1**),
 - b. A pink iPhone model A1784 contained in a clear case two black circles, belonging to Charles BALDWIN (**SUBJECT ELECTRONIC DEVICE 2**),
 - c. A silver iPhone SE, belonging to Charles BALDWIN (**SUBJECT ELECTRONIC DEVICE 3**),
 - d. A white iPhone bearing serial number: 352889115890956, belonging to Charles BALDWIN (**SUBJECT ELECTRONIC DEVICE 4**).

- e. A blue Samsung cellular phone bearing serial number: 353290110592953, belonging to Charles BALDWIN (**SUBJECT ELECTRONIC DEVICE 5**),
- f. A black Samsung Smartphone, belonging to Charles BALDWIN (**SUBJECT ELECTRONIC DEVICE 6**),
- g. A white iPhone bearing serial number: 354910095740702, contained in a purple cell phone case, belonging to Leah THOMPSON (**SUBJECT ELECTRONIC DEVICE 7**),

which are each also described in Attachment A-1 and collectively referred to as the **SUBJECT ELECTRONIC DEVICES**, for the items and information more fully described in Attachment B-1; and

- h. A 2000 gold Chrysler Town and Country, bearing South Carolina registration SFR-178, and VIN:1C4GP54L9YB593093 (the “**TARGET VEHICLE**”), further described in Attachment A-2, to seize the items described in Attachment B-2.

2. Based on the facts set forth in this affidavit, I respectfully submit that there is probable cause to believe that the **SUBJECT ELECTRONIC DEVICES** and the **TARGET VEHICLE** contains evidence, fruits, and instrumentalities of distribution and possession with intent to distribute controlled substances, in violation of 21 U.S.C. § 841, conspiracy to distribute controlled substances, in violation of 21 U.S.C. § 846, and possession of a firearm in furtherance of a drug trafficking crime, in violation of 18 U.S.C. § 924(c).

AFFIANT BACKGROUND

3. I have been a SA with the ATF since April 2020. I am assigned to the Baltimore Field Division, Baltimore Group II. I have received training through the Federal Law Enforcement

Training Center, located in Glynco, Georgia, to include the Criminal Investigator Training Program, the ATF Special Agent Basic Training Program. Prior to being a SA with the ATF, I was a SA with Homeland Security Investigations in New York City for two years.

4. I have been involved in multiple investigations involving firearms violations, domestic and international narcotics violations, and violent crimes. During these investigations, I have conducted surveillance of numerous drug dealers. I have also interviewed drug dealers, users, and confidential informants where I discussed with these individuals the life-style, appearance, and habits of drug dealers and users. I have examined records of, among others, buyers and sellers' lists and pay/owe ledgers. I have participated in the execution of several search and seizure warrants on, for example, warrants to search residences, stash houses, social media accounts, cellphone contents, and vehicles. I have also participated in wiretap investigations. I have assisted in controlled purchase operations involving confidential informants and undercover agents/officers. I have listened to and interpreted recorded conversations between drug dealers and their co-conspirators. I have been the affiant on more than 50 search and seizure warrants.

5. Through my training and experience, I know the habits, methods, routines, practices, and procedures commonly employed by persons who commit violent acts, possess firearms illegally, and traffic controlled substances. Based upon my training and experience, I have learned the following:

- a. Illegal narcotics trafficking (and the possession of firearms in connection with that trafficking) is an ongoing and recurring criminal activity. As contrasted with crimes against persons, which tend to be discrete offenses, narcotics trafficking is a commercial activity that is characterized by regular, repeated criminal activity.
- b. Cellphones are an indispensable tool of the illegal narcotics trafficking trade. Traffickers use cellphones, push-to-talk phones, Short Message Service (SMS), electronic-mail, and similar electronic means and/or devices, often under fictitious names or names other than their own, to maintain contact with

other conspirators and traffickers. In addition, illegal narcotics traffickers will often change their cellphones following the arrest of a member of their drug trafficking organization (DTO), or at random to frustrate law enforcement efforts.

- c. Illegal narcotics traffickers use cellphones and other electronic communications devices to facilitate illegal transactions. The electronically stored information on these devices is of evidentiary value in identifying other members of the trafficking conspiracy and establishing the relationship between these individuals, including photographs and other identifying information stored on these devices; they also use their cellphones to communicate on various social media platforms such as Facebook and Instagram.
- d. Persons who commit violent acts, possess firearms illegally, and traffic narcotics use computers or other electronic storage media, including smart phones, to store the records documents, take and store photographs and videos of co-conspirators, and contraband.
- e. Illegal narcotics traffickers keep and maintain narcotics, firearms, and records of their various activities. Such items are regularly concealed in a suspect's automobile, residence, office, and on his person, and that they take various forms. Documents commonly concealed by traffickers, include but are not limited to notes in code, deposit slips, wired money transactions, hidden bank accounts, photographs of co-conspirators, various forms of commercial paper, personal address books, notebooks, records, receipts, ledgers, travel receipts (rental receipts, airline tickets, bus tickets, and/or train tickets) both commercial and private, money orders and other papers relating to the ordering, transportation, sale and distribution of controlled dangerous substances or other such documents which will contain identifying data on the co-conspirators. These items are kept in locations that are considered safe by the traffickers such as safety deposit boxes, residences, vehicles and on their person, where they have ready access to them. Narcotics traffickers often have several residences decreasing the likelihood of detection by law enforcement.
- f. Those who engage in illegal narcotics trafficking will maintain large amount of cash to finance their ongoing business. The also often possess paraphernalia used in the manufacturing, packaging, preparing, and weighing of illegal narcotics. These items are frequently kept where the traffickers have ready access to them, including in their residences and vehicles.
- g. Illegal narcotics traffickers often possess and use of firearms to protect their narcotics, proceeds, and territory where they sell the narcotics from rivals and potential robbers. They keep these firearms in places where they have ready access to them, including in their residences and vehicles.

6. I have set forth only the facts I believe necessary to establish probable cause for the requested warrants. I have not, however, excluded information known to me that would defeat probable cause. The information contained in this affidavit is based upon my personal knowledge, my review of documents and official police reports, interviews with witnesses and other evidence and my conversations with other law enforcement officers and other individuals. All conversations and statements described in this affidavit are related in substance and in part unless otherwise indicated.

PROBABLE CAUSE

7. On July 23, 2021, the Honorable Thomas M. DiGirolamo of the District of Maryland issued a federal search warrant for the residence of 745 North Grantley Street, Baltimore, Maryland 21229 (the “Grantley Street Address”).¹ Charles BALDWIN and Kevin BALDWIN were the targets of the warrant. The Affidavit in support of the search warrant for the Grantley Street Address is attached to this Affidavit as Exhibit A.

8. On July 26, 2021, at 6:00 a.m., the ATF, U.S. Marshal Service (“USMS”), and the Federal Bureau of Investigations (“FBI”) executed the search warrant at the Grantley Street Address. Overall, investigators found three firearms—a Springfield XD45, .45 caliber pistol, with an obliterated serial number, a Rossi 38 special revolver bearing a serial number J124634, a Ruger, 5.56 caliber, and an AR-style rifle, bearing serial number 857-20170—in the basement of the residence. Also found in both the upstairs living room and the basement were assorted magazines, ammunition, drug packaging material, and a distribution amount of suspected Fentanyl (contained in two separate clear sandwich bags). The **SUBJECT ELECTRONIC DEVICES** were also

¹ Case No. 1:21-mj-2155 TMD.

located in various places in the residence, as described below.

9. Investigators located six individuals in the residence: Charles BALDWIN, Mizell TAYLOR, Leah THOMPSON, WB, LB, and TB.²

10. Upon USMS advising all occupants to exit the residence, an unidentified individual attempted to exit the rear basement door. USMS could not identify who it was, and no occupants that had been detained admitted to being the one that attempted to exit out of the basement door. Investigators asked all occupants of the residence if anyone was still located in the residence and what their location in the residence was during the execution of the search and seizure warrant. This was done to determine if an individual was still barricaded in the basement of the residence.

11. TAYLOR then told investigators he had been sleeping on the couch in the living room, and he had run into the basement when the police attempted to make entry into the residence. LB and TB were both located in the upstairs of the residence. Charles BALDWIN, THOMPSON, and WB were all located in the basement of the residence.

12. Investigators seized **SUBJECT ELECTRONIC DEVICE 1** from the couch located in the living room of the residence, where TAYLOR stated he had been sleeping. TAYLOR identified **SUBJECT ELECTRONIC DEVICE 1** as his device, after asking investigators if he could have his cellphone. Several items were found in close proximity to the couch where TAYLOR was sleeping, including a magazine with ammunition, a scale, and drug packaging paraphernalia, commonly used to package a larger quantity of illegal narcotics into individual user quantities for sale.

13. Investigators seized **SUBJECT ELECTRONIC DEVICES 2-7** (the remaining

² This Affidavit uses the initials of these three individuals because they are not the targets/subjects of the Application and Affidavit for a Search Warrant.

cellphones) from the basement of the residence. Charles BALDWIN identified the basement room as his bedroom. THOMPSON also advised investigators that the basement of the residence was Charles BALDWIN's bedroom.

14. Investigators showed Charles BALDWIN **SUBJECT ELECTRONIC DEVICE 4**, which was found on the bed in the basement of the residence, and he identified **SUBJECT ELECTRONIC DEVICE 4** as his cellular phone and further stated that he had several cellphones in the basement. Thompson told investigators that she possessed an iPhone with a purple case which was located in the basement. Investigators also recovered **SUBJECT ELECTRONIC DEVICES 2, 3, 5, 6, and 7** from the basement bedroom of residence. After Thompson asked investigators for her cell phone, she identified **SUBJECT ELECTRONIC DEVICE 7**, which had a purple case, as her cellular device. As stated above, the basement is also where firearms, several rounds of assorted ammunition and magazines, illegal narcotics, and narcotics paraphernalia including plastic baggies used to package user quantities of illegal narcotics (which are commonly referred to as zips) were found. I know based on my training and experience that these small baggies are used to package into individual units of various types of illegal narcotics including heroin, crack-cocaine, and powdered cocaine.

15. As described in the Affidavit in support of the search warrant for the Grantley Street Address, see Exhibit A, investigators had information that Charles BALDWIN and Kevin BALDWIN were selling illegal narcotics and using the Grantley Street Address to do so. Investigators found mail at the residence on Grantley Street, in the name of Kevin BALDWIN, including a letter from the White House, signed by President Biden, in reference to Kevin BALDWIN's stimulus check. Given this prior information and the narcotics and paraphernalia found in the residence, I believe based on my training and experience that the firearms in the

residence were there to protect a narcotics trafficking business. I further believe based on my training and experience that the evidence found in the residence—firearms, ammunition, materials used to prepare and package narcotics (including plastic baggies used to package larger quantities of illegal narcotics into user quantities of illegal narcotics for the purpose of sale), a scale, and distribution levels of narcotics—indicates that the Grantley Street Address was being used to store, protect, prepare, and package narcotics for sale. I know based on my training and experience that this type of residence is often referred to as a “stash house.”

16. I believe that **SUBJECT ELECTRONIC DEVICES 2-6**, believed to belong to Charles BALDWIN, are likely to contain evidence of his narcotics trafficking activities based on all the evidence discussed in this Affidavit and the Affidavit for the Grantly Street Address (Exhibit A), and because, as described above, narcotics traffickers’ often keep multiple phones and use those phones to conduct and store information relating to their illegal business. Also, given that TAYLOR and THOMPSON were both located in the “stash house,” that THOMPSON attempted to flee when investigators arrived, and their cellphones were found close to the narcotics distribution items, I believe these individuals were also part of the narcotics distribution activities and their cellphones, **SUBJECT ELECTRONIC DEVICES 1 and 7** will contain evidence of drug trafficking.

17. The **SUBJECT ELECTRONIC DEVICES** are currently in the custody of the ATF at the ATF Baltimore Strike Force office.

18. The **TARGET VEHICLE** was parked in front of the Grantley Street Address during the execution of the search warrant. Homeland Security Investigations (HSI) Task Force Officer (“TFO”) and Baltimore Police Department (“BPD”) detective Donald Hayes and his police dog (K9 “Bella”) conducted an exterior scan of the vehicle. K9 “Bella” is trained to detect the odor

of controlled dangerous substances.³ These controlled dangerous substances include heroin, black tar heroin, cocaine and marijuana. Upon detection of any of these four controlled dangerous substances odors, K-9 “Bella’s” behavior will change. K-9 “Bella” is trained to come to a final response by passively sitting at the source of the odor. This is called a “passive” final response. This response may also indicate items recently contaminated with, or associated with, the odor of one or more of the aforementioned controlled dangerous substances. On this occasion, K9 “Bella” alerted to the presence of a controlled dangerous substance in the **TARGET VEHICLE**. The **TARGET VEHICLE** was subsequently towed to the BPD Northern District at 2201 West Cold Spring Lane, Baltimore, Maryland 21209, where the **TARGET VEHICLE** is currently being stored.

19. A South Carolina Motor Vehicle Administration database check revealed that the vehicle is registered to Brianna Ard. On October 28, 2020, Charles BALDWIN was the victim of a non-fatal shooting in the 3600 block of 5th street, Brooklyn, Maryland. As a result of investigation, BPD seized two cellular phones belonging to Charles BALDWIN. Investigators found a piece of paper folded in the phone case of one of the cellular phones recovered. The piece of paper stated “I Derrick Dedeaux Brianne Ard, sold this van 2000 Town & country to this buyer Kevin Baldwin for \$450.00 on this date Oct. 3 2020. Phone number 404 576 4626 He will have the title on Oct 4 2020.” In the top right corner of the document the word bill of sale is written, on the bottom right side of the document it is signed Derrick Dedeux.

³ Detective/TFO Hayes and his K-9 partner “Bella” have completed an eight-week drug detection canine course with the BPD and “Bella” is certified in the detection of heroin, cocaine and marijuana by the BPD K-9 Training Unit as of 7/7/2016. Additionally, the BPD requires that all K-9 handlers and canines to go through annual recertification and training at a frequency of two days per month. K-9 “Bella’s” last annual certification date was 4/29/2021.

20. I know that Kevin BALDWIN is Charles BALDWIN's brother through physical surveillance, social media, and information from confidential sources, as described in the Affidavit in support of the search warrant for the Grantley Street Address. *See* Exhibit A.

21. After the execution of the search warrant, BPD charged Charles BALDWIN with assault weapon possession/sell, reg firearm: Stolen/sell ETC, known alter firearm ID number, and body armor-may not possess. BPD charged TAYLOR with, assault weapon poss/sell, Reg firearm: illegal Possession, RFL/shotgun poss-disqual, reg firearm: stolen/sell etc, known alter firearm ID number, illegal poss ammo, poss of firearm minor x3, and body armor- may not poss. BPD charged WB with assault weapon poss/sell, reg firearm: stolen/sell, known alter firearm ID number, and body armor- may not poss.

22. On July 29, 2021, at approximately 5:42 p.m. Charles BALDWIN called on the telephone number 240-229-8045 on a recorded jail telephone (which tells the users that the call will be recorded and monitored). On this call, Charles BALDWIN was heard talking to Yolanda Budd, who I know to be Charles BALDWIN's mother. Further, during the execution of the search and seizure warrant at the Grantley Street Address, Budd arrived at the residence and provided that telephone number (240-229-8045) to investigators. During the call, Charles BALDWIN told Budd to sell his van. Budd replied that "they" "took" the van, which I believe was Budd telling Charles BALDWIN that investigators towed his van. The **TARGET VEHICLE** is the only vehicle investigators towed so I believe that Charles BALDWIN was telling his mother to get rid of the **TARGET VEHICLE**, likely because it contained evidence of illegal activity. This also leads me to believe that Charles BALDWIN and Kevin BALDWIN shared possession of the **TARGET VEHICLE**.

BACKGROUND CONCERNING ELECTRONIC COMMUNICATIONS DEVICES

23. The fruits and instrumentalities of criminal activity are often concealed in digital form. Furthermore, digital camera technology is often used to capture images of tools and instrumentalities of pending criminal activity. The **SUBJECT ELECTRONIC DEVICES** have both digital storage capacity and digital camera capabilities.

24. Individuals engaged drug trafficking offenses often use cell phones to communicate with suppliers, to place orders with suppliers, to communicate with customers, to receive orders from customers, and to arrange meeting times and locations for the distribution of controlled substances. The individuals engaging in drug trafficking will often use a combination of voice calls and text messages to coordinate drug transactions. Individuals engaged in drug trafficking offenses also use digital storage devices to maintain telephone number “contact lists” of individuals who may have assisted in the planning of this and other criminal activity.

25. Narcotic traffickers often place nominal control and ownership of telephones in names other than their own to avoid detection of those telephones by government agencies. Even though telephones are in the names of other people, drug traffickers retain actual ownership, control, and use of the telephone, exercising dominion and control over them.

26. Drug traffickers utilize different types of communication devices, and change the numbers to these communication devices frequently. This is done to avoid detection by law enforcement personnel. Also, as noted above, drug traffickers dedicate different communication devices for different aspects of the trafficking organization.

27. Cellular phones associated with drug traffickers include various types of evidence. Phones may contain relevant text messages or other electronic communications; they may contain electronic address books listing the phone numbers and other contact information associated with

co-conspirators; and they may contain other types of information.

28. Drug traffickers often take photos of themselves with large quantities of controlled substances, money, or high-end consumer items, like cars or watches. Further, those who possess firearms also often take photos of the firearms and/or themselves with the firearms. These “trophy” photos are often maintained on cellular telephones to be shared on social media, or as symbols of their success.

29. Finally, the mere fact of a cellular phone’s call number, electronic serial number or other identifying information may be of evidentiary value as it may confirm that a particular cell phone is the phone identified during a wiretap, pen register, or other electronic investigation.

FORENSIC ANALYSIS OF ELECTRONIC COMMUNICATIONS DEVICES

30. Based on my training and experience, I know that electronic devices such as cellular phones (smartphones) can store information for long periods of time. Similarly, things that have been viewed via the internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools. There is probable cause to believe that things that were once stored on the **SUBJECT ELECTRONIC DEVICES** may still be stored on those devices, for various reasons, as discussed in the following paragraphs.

31. As further described in Attachment B-1, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **SUBJECT ELECTRONIC DEVICES** were used, the purpose of its use, who used it, and when.

32. There is probable cause to believe that this forensic electronic evidence might be on the **SUBJECT ELECTRONIC DEVICES** because data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of

a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

33. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

34. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

35. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

36. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a

storage medium.

37. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

38. During this case and in numerous others involving complex DTOs, investigators have learned that the drug-trafficking organization relies heavily on electronic devices to facilitate drug trafficking. It is necessary to conduct a physical inspection of the electronic devices in order to obtain electronic communications and other information that might be stored on the seized phones and to determine whether any of the seized phones were the subject of wiretap, pen register or other investigation detailed herein. The phones may also contain data and communications that were not electronically intercepted due to encryption or for other reasons.

39. Again, the **SUBJECT ELECTRONIC DEVICES** remain in the custody of law enforcement. The only known specifics of each phone requested for authorization to search are detailed in Attachment A-1 and the types of information expected to be recovered from the devices are listed in Attachment B-1.

CONCLUSION

40. Accordingly, there is probable cause to believe that evidence will be found from an analysis of the recovered **SUBJECT ELECTRONIC DEVICES**. The **SUBJECT ELECTRONIC DEVICES** may contain the records of the most recent calls, which may include calls with persons involved in the offense(s). The **SUBJECT ELECTRONIC DEVICES** may contain copies of SMS or text or other electronic communications relating to activities associated with the offense(s). The **SUBJECT ELECTRONIC DEVICES** may also contain a variety of

other electronic evidence, including electronic communications through various cellular or internet-based applications, photographs and other information. I respectfully request that this Court issue a search warrant for the **SUBJECT ELECTRONIC DEVICES**, and authorize the search of the items described in Attachment A-1, for the information set forth in Attachment B-1, where applicable, which constitute fruits, evidence and instrumentalities of conspiracy to distribute controlled substances, in violation of 21 U.S.C. § 846, possession with intent to distribute controlled substances, in violation of 21 U.S.C. § 841, and possession of a firearm in furtherance of a drug trafficking crime, in violation of 18 U.S.C. § 924(c).

41. Further, I respectfully request that this Court issue a search warrant for the **TARGET VEHICLE**, described in Attachment A-2, for the items set forth in Attachment B-2, which will constitute evidence, fruits, and instrumentalities of conspiracy to distribute controlled substances, in violation of 21 U.S.C. § 846, possession with intent to distribute controlled substances in violation of 21 U.S.C. § 841, and possession of a firearm in furtherance of a drug trafficking crime, in violation of 18 U.S.C. § 924(c).

REQUEST FOR NIGHT-TIME AUTHORIZATION

42. There is good cause for the Court to authorize the requested searches at any time of the day or night. The **SUBJECT ELECTRONIC DEVICES** and the **TARGET VEHICLE** are already in law enforcement custody, and it is reasonable to allow law enforcement to execute the requested searches at any hour of the day, even during the evening or night, if doing so is convenient for the investigators or examiners. Because the **SUBJECT ELECTRONIC DEVICES** and the **TARGET VEHICLE** are already in law enforcement custody, there will be no prejudice to any other person from this request.

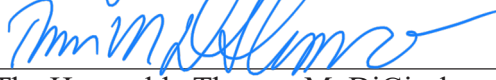
43. I declare under the penalty of perjury that the foregoing is true and correct to the best of my knowledge.

JOSHUA. FUTTER

Digitally signed by JOSHUA.
FUTTER
Date: 2021.08.11 17:31:02 -04'00'

Special Agent Joshua Futter
ATF

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this day of August 13, 2021.



The Honorable Thomas M. DiGirolamo
United States Magistrate Judge

ATTACHMENT A-1
Device to be Searched

1. A black iPhone contained in a clear phone case with stickers on it, belonging to Mizell TAYLOR (**SUBJECT ELECTRONIC DEVICE 1**).
2. A pink iPhone model A1784 contained in a clear case two black circles, belonging to Charles BALDWIN (**SUBJECT ELECTRONIC DEVICE 2**).
3. A silver iPhone SE, belonging to Charles BALDWIN (**SUBJECT ELECTRONIC DEVICE 3**).
4. A white iPhone bearing serial number: 352889115890956, belonging to Charles BALDWIN (**SUBJECT ELECTRONIC DEVICE 4**).
5. A blue Samsung cellular phone bearing serial number: 353290110592953, belonging to Charles BALDWIN (**SUBJECT ELECTRONIC DEVICE 5**).
6. A black Samsung Smartphone, belonging to Charles BALDWIN (**SUBJECT ELECTRONIC DEVICE 6**).
7. A white iPhone bearing serial number: 354910095740702, contained in a purple cell phone case, belonging to Leah THOMPSON (**SUBJECT ELECTRONIC DEVICE 7**).

Each of the **SUBJECT ELECTRONIC DEVICES** is currently in the custody of the ATF at the Baltimore Strike Force office.

ATTACHMENT A-2

Item(s) to be searched

The **TARGET VEHICLE** is a 2000 gold Chrysler Town and Country, bearing South Carolina registration SFR-178, and VIN:1C4GP54L9YB593093. Below are two photos of the **TARGET VEHICLE**.



ATTACHMENT B-1

Items to be Seized

All records contained in the items described in Attachment A-1, which constitute evidence of violations of 21 U.S.C. §§ 846 and 841 and 18 U.S.C. § 924(c) including but not limited to that outlined below, for each of the **SUBJECT ELECTRONIC DEVICES**,

1. All evidence of firearms and narcotic possession; narcotic distribution; and co-conspirators and/or associations to same.
2. Contact logs that refer or relate to the user of any and all numbers on the **SUBJECT ELECTRONIC DEVICE**.
3. Call logs reflecting date and time of received calls.
4. Any and all digital images and videos of persons associated with this investigation.
5. Text messages to and from the **SUBJECT ELECTRONIC DEVICE** that refer or relate to the crimes under investigation.
6. Records of incoming and outgoing voice communications that refer or relate to the crimes under investigation.
7. Voicemails that refer or relate to the crimes under investigation.
8. Voice recordings that refer or relate to the crimes under investigation.
9. Any data reflecting the phone's location.
10. Contact lists.
11. Any and all records related to the location of the user(s) of the **SUBJECT ELECTRONIC DEVICE**.
12. For each of the **SUBJECT ELECTRONIC DEVICES**:
 - a. Evidence of who used, owned, or controlled the **SUBJECT ELECTRONIC DEVICE** at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the **SUBJECT ELECTRONIC DEVICE**, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the **SUBJECT ELECTRONIC DEVICE** of other storage devices or similar containers for electronic evidence;
- e. evidence of counter forensic programs (and associated data) that are designed to eliminate data from the **SUBJECT ELECTRONIC DEVICE**;
- f. evidence of the times the **SUBJECT ELECTRONIC DEVICE** was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the **SUBJECT ELECTRONIC DEVICE**;
- h. documentation and manuals that may be necessary to access the **SUBJECT ELECTRONIC DEVICE** or to conduct a forensic examination of the **SUBJECT ELECTRONIC DEVICE**; and,
- i. contextual information necessary to understand the evidence described in this attachment.

With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

- 1. surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);
- 2. “opening” or cursorily reading the first few “pages” of such files to determine their precise contents;
- 3. “scanning” storage areas to discover and possibly recover recently deleted files;
- 4. “scanning” storage areas for deliberately hidden files; or
- 5. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file or storage area, shall cease.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated, absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

ATTACHMENT B-2

Item's to be seized

1. Any narcotics and any records of narcotics transactions including, but not limited to, books, ledgers, receipts, notes, and other papers relating to the manufacture, transportation, possession, and distribution of controlled substances;
2. Financial instruments and records and other records or documents relating to narcotics-trafficking activity or the disposition of narcotics proceeds, including, but not limited to, currency, bank checks, cashiers checks, Western Union receipts, money orders, stocks, bonds, precious metals, and real estate records.
3. Records that identify other co-conspirators, including, but not limited to: address books, telephone books, rolodexes, telephones, pagers, or personal digital assistants with stored telephone information, notes reflecting telephone and pager numbers, photographs (to include still photos, negatives, movies, slides, video tapes, and undeveloped film), and audiotape recordings of conversations, including those made over telephone answering machines;
4. Cellular telephones, pagers and records and receipts reflecting their ownership and use;
5. Documents or other records relating to state court proceedings involving other co-conspirators, including, but not limited to, charging documents and bail records;
6. Identification documents;
7. Records of travel including, but not limited to, tickets, transportation schedules, passports, notes and receipts related to travel, and motel/hotel receipts;
8. Indicia of ownership of the vehicle, including keys, photographs, or documents;
9. United States currency, precious metals, jewelry and financial instruments, stocks and bonds;
10. Safes, combination or key-lock strong boxes or other secure storage containers, suitcases, locked cabinets and other types of locked or closed containers, and hidden compartments that may contain any of the foregoing.
11. Firearms, ammunition, and any records pertaining to firearms, or the transaction of firearms.
12. Computer(s), computer hardware, software, related documentation, passwords, data security devices (as described below), videotapes, and or video recording devices, and data that may constitute instrumentalities of, or contain evidence related to the specified criminal offenses. The following definitions apply to the terms as set out in this affidavit and attachment:

- a. Computer hardware: Computer hardware consists of all equipment, which can receive, capture, collect analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Hardware includes any data-processing devices (including but not limited to cellular telephones, central processing units, laptops, tablets, eReaders, notes, iPads, and iPods; internal and peripheral storage devices such as external hard drives, thumbdrives, SD cards, flash drives, USB storage devices, CDs and DVDs, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, and related communications devices such as cables and connections), as well as any devices mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).
- b. Computer software is digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- c. Documentation: Computer-related documentation consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, software, or other related items.
- d. Passwords and Data Security Devices: Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touches. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

As used above, the terms “records, documents, messages, correspondence, data, and materials” includes records, documents, messages, correspondence, data, and materials, created, modified or stored in any form, including electronic or digital form, and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of computer hardware, software, documentation, passwords, and/or data security devices.

13. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:
- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - f. evidence of the times the COMPUTER was used;
 - g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - i. contextual information necessary to understand the evidence described in this attachment.

With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

1. surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);
2. “opening” or cursorily reading the first few “pages” of such files in order to determine their precise contents;
3. “scanning” storage areas to discover and possibly recover recently deleted files;
4. “scanning” storage areas for deliberately hidden files; or
5. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.
6. If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file or storage area, shall cease.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.